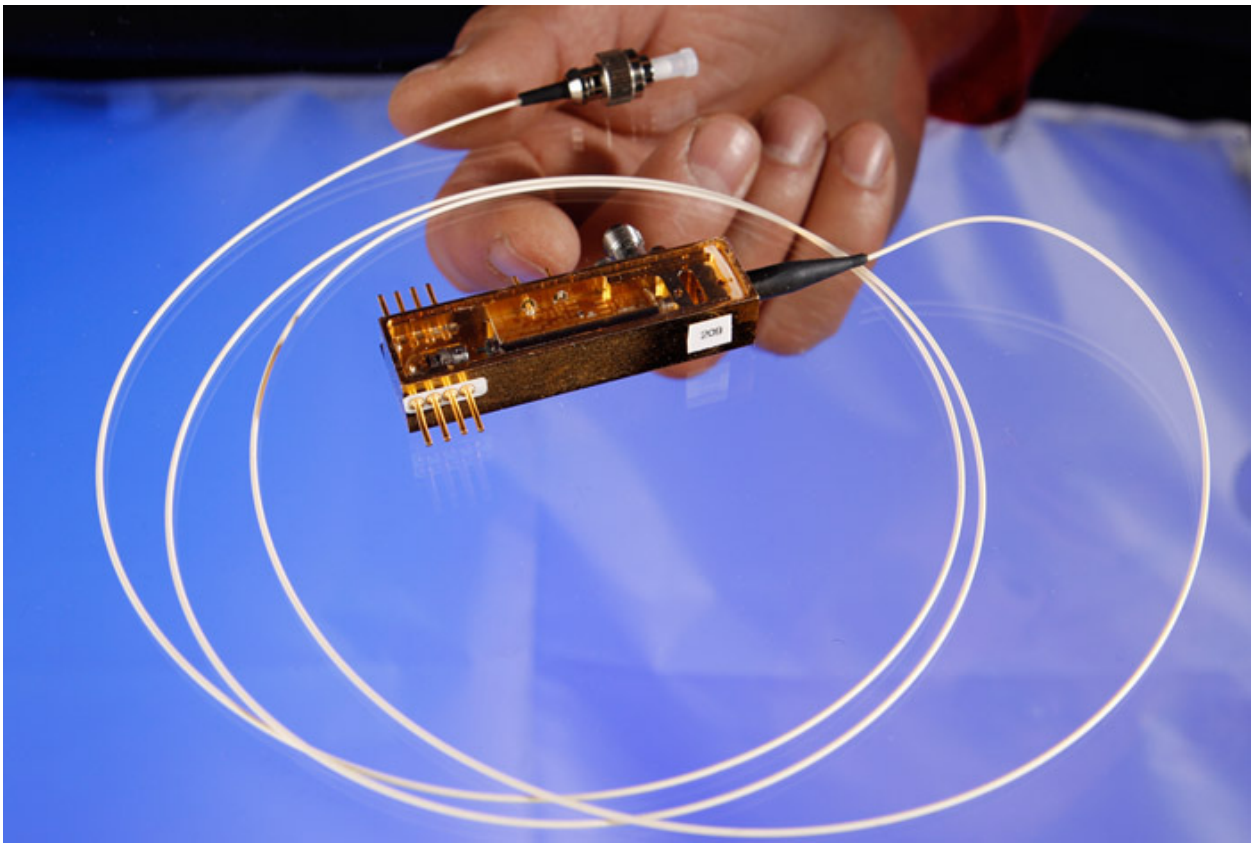
Quantum cryptography put to work for electric grid security

February 14, 2013



LOS ALAMOS, N.M., Feb. 14, 2013—Recently a Los Alamos National Laboratory quantum cryptography (QC) team successfully completed the first-ever demonstration of securing control data for electric grids using quantum cryptography.

The demonstration was performed in the electric grid test bed that is part of the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project at the University of Illinois Urbana-Champaign (UIUC) that was set up under the Department of Energy's Cyber Security for Energy Delivery Systems program in the Office of Electricity Delivery and Energy Reliability.

Novel methods for controlling the electric grid are needed to accommodate new energy sources such as renewables whose availability can fluctuate on short time scales. This requires transmission of data to and from control centers; but for grid-control use, data must be both trustworthy and delivered without delays. The simultaneous requirements

of strong authentication and low latency are difficult to meet with standard cryptographic techniques. New technologies that further strengthen existing cybersecurity protections are needed.

Quantum cryptography provides a means of detecting and defeating an adversary who might try to intercept or attack the communications. Single photons are used to produce secure random numbers between users, and these random numbers are then used to authenticate and encrypt the grid control data and commands. Because the random numbers are produced securely, they act as cryptographic key material for data authentication and encryption algorithms.

At the heart of the quantum-secured communications system is a unique, miniaturized QC transmitter invention, known as a QKarD, that is five orders of magnitude smaller than any competing QC device. Jane Nordholt, the Los Alamos principal investigator, put it this way: “This project shows that quantum cryptography is compatible with electric-grid control communications, providing strong security assurances rooted in the laws of physics, without introducing excessive delays in data delivery.”

A late-2012 demonstration at UIUC showed that quantum cryptography provides the necessary strong security assurances with latencies (typically 250 microseconds, including 120 microseconds to traverse the 25 kilometers of optical fiber connecting the two nodes) that are at least two orders of magnitude smaller than requirements. Further, the team’s quantum-secured communications system demonstrated that this capability could be deployed with only a single optical fiber to carry the quantum, single-photon communications signals; data packets; and commands. “Moreover, our system is scalable to multiple monitors and several control centers,” said Richard Hughes, the co-principal investigator from Los Alamos.

The TCIPG cyber-physical test bed provides a realistic environment to explore cutting-edge research and prove emerging smart grid technology in a fully customizable environment. In this demonstration, high-fidelity power simulation was leveraged using the real-time digital simulator to enable hardware in the loop power simulation to drive real phasor measurement units (PMUs), devices, deployed on today's electric grid that monitor its operation.

“The simulator provides a mechanism for proving technology in real-world scenarios,” said Tim Yardley, assistant director of test bed services. “We're not just using perfect or simulated data, so the results demonstrate true feasibility.”

The power simulation was running a well-known power-bus model that was perturbed by introducing faults, which drove the analog inputs on the connected hardware PMU. The PMU then communicated via the standard protocol to the quantum cryptography equipment, which handled the key generation, communication and encryption/decryption of the connection traversing 25 kilometers of fiber. A phasor data concentrator then collected and visualized the data.

“This demonstration represents not only a realistic power model, but also leveraged hardware, software and standard communication protocols that are already widely deployed in the energy sector,” said William H. Sanders, the Donald Biggar Willett Professor of Engineering at UIUC and principal investigator for TCIPG. “The success of the demonstration emphasizes the power of the TCIPG cyber-physical test bed and the strength of the quantum cryptography technology developed by Los Alamos.”

The Los Alamos team submitted 23 U. S. and foreign patent applications for the inventions that make quantum-secured communications possible. The Los Alamos

Technology Transfer Division has already received two licensing inquiries from companies in the electric grid control sector, and the office plans an industry workshop for early 2013 when the team's patents will be made available for licensing.

The Los Alamos team is seeking funding to develop a next-generation QKarD using integrated electro-photonics methods, which would be even smaller, more highly integrated, and open the door to a manufacturing process that would result in much lower unit costs.